FAULT TOLERANT QUANTUM COMPUTING: DIAGRAMMATIC APPROACHES

A Synopsis

Submitted in the partial fulfillment of the requirements for the

degree of

Doctor of Philosophy

in

Physics

Submitted by

Akalank jain

Dr. Shiroman Prakash	Prof. G.S. Tyagi	Prof. G.S. Tyagi
Supervisor	Head	Dean
Department of Physics	Department of Physics	Department of Physics

Department of Computer Science and Physics

Faculty of Science

Dayalbagh Educational Institute (Deemed University)

Dayalbagh, Agra-282005

March, 2017.

INTRODUCTION AND LITERATURE REVIEW

Quantum computing

Let us give a brief history of the early development of quantum computing.

Quantum mechanical systems might be able to solve certain complex problems faster than classical systems. Feynman first suggested the possibility of a quantum computer in a talk in 1981 [1]. In 1982, P. Benioff published an article titled “Quantum mechanical models: Turing machines that dissipate no energy” [2] which also described a quantum computer early on.

The computational power of a quantum computer is at least that of a classical computer. But quantum computation appears able to solve some problems much faster than classical computation. In a 1985 paper by David Deutsch titled “Quantum theory, the Church-Turing principle and the Universal Quantum Computer” [3], Deutsch argued that a quantum computer can perform certain tasks quickly that a classical Turing machine cannot perform quickly — namely, parallel calculation in a single register and perfect simulation. (Though from the point of view of computability only, both are equally powerful.)

In 1989, Deutsch wrote the paper “Quantum computational networks”, [4] in which he showed quantum gates can be used for quantum computation in similar manner as classical logic gates can be used for classical computation.

In a 1993 paper published by Andrew Chi Chih Yao [5], it was shown that computation of any function in polynomial time by a Turing machine can also be done using quantum circuits. In 1993, Ethan Bernstein and Umesh Vazirane [6] showed that a quantum Turing machine can efficiently simulate any Turing machine and this paper is vital to quantum complexity theory.

One might ask what are the minimal ingredients, i.e., gates, needed to implement a quantum computer. In 1995, Adrino Barenco, in “Elementary gates for quantum computation” [7], showed that we were able to make any circuit using combinations of single-qubit and controlled exclusive OR gates on two qubits. David DiVicenzo, in “Two qubit gates are universal for quantum computation”, [8] showed that two-qubit quantum gates are sufficient. Adriano Barenco, David Deutsch and Artur Ekert, in “Conditional quantum dynamics and logic gates” [9], showed that a combination of quantum controlled-NOT gates and on electron qubit gates are sufficient. Seth Lloyd, in “almost any quantum logic gate is universal” [10], showed that nearly all quantum gates with two or more inputs are universal.

Quantum Algorithms

In 1992, David Deutsch and Richard Jozsa published “Rapid solution of problems by quantum computation” [11]. They developed an algorithm for determining if a function is constant or balanced. This algorithm, called the Deutsch-Jozsa algorithm, is the first quantum algorithm which works faster than any classical algorithm for a specific problem.

Bernstein and Vazirani [6], first recognized a problem that can be solved in polynomial time by quantum algorithm but needs superpolynomial time classically.

In 1993, Charles H Bennett *et al.* wrote “Teleportation an unknown quantum state via dual classical and Einstein-Podolsky Rosen Channels” [25]. Later, In 1997, Dik Bouwmeester *et al.* produced “Experimental quantum teleportation”.

Then, In 1994 Shor published a quantum algorithm for efficient integer factoring [13, 14]. This algorithm initiated an immortal interest to build a quantum computer. Integer factorizing is seemingly impossible using classical computer within a reasonable time. If physicists and

computer scientists successfully constructed such a device, then several widely-used public key cryptography methods, e.g., RSA encryption, could be broken. [15]

After Shor's 1994 publication the following new applications came into the picture:

(1.) Database searching [16]

(2.) Machine learning tasks [17]

(3.) Techniques for simulation of quantum systems [18]

While quantum computing has tremendous applications, it appears extremely difficult to construct a quantum computer.

Fault tolerant quantum computing

Decoherence, or noise from the environment, is the major obstacle to constructing a large-scale working quantum computer. While classical information can be protected from errors by multiple copies, in quantum mechanics, the no-cloning theorem forbids cloning of quantum information. Therefore some critics once thought that quantum error-correction was impossible, and a quantum computer could not be built in practice.

In 1995 Peter Shor's article "Scheme for reducing decoherence in computer memory" [19] revealed that to provide some protection from errors, each qubit can be encoded into nine qubits. Independently, Andrew M. Steane wrote "Error correction codes in quantum theory" [20] which also describes another quantum error correcting code. After a while Shor and A.R. Calderbank released "Good quantum error correcting codes exist" [21], which established the theory of quantum error correction.

Hence Shor, Steane and Calderbank found a way to protect quantum information from errors, thereby making a quantum computer possible.

Our aim is not only to reduce the error rate but also to minimize the number of extra bits stored or transmitted. The father of information theory, Claude E. Shannon [22] released "A mathematical theory of communication", in which he addressed this problem for classical information. After five decades, Benjamin Schumacher generalized Shannon's idea to the quantum case and published "Quantum coding" [23] and also produced "A new proof of the quantum noiseless coding theorem" [24], which helped begin the theory of quantum information.

Fault tolerant quantum computing was introduced by Daniel Gottesman, working under John Preskill. It shows how gates can be implemented in a way such that errors from faulty gates do not build up.

Typically, only a certain discrete subset – such as the Clifford group – can be realized in a fault-tolerant way. This gate set is not universal, and must be supplemented by additional gates, such as T gates, which are costlier to implement, in order to achieve universal quantum computation.

Details of error-correcting codes and fault tolerant schemes depend crucially on the dimension of the quantum systems used to store information. For example, the smallest error-correcting code for a three-single state quantum system, qutrits, require only three physical qutrits to encode a logical qutrit, while the smallest single qubit error-correcting code require 5 physical qubits for encoding one logical qubit. See [40] for more on qudits of odd prime dimension.

Error-correcting codes and fault tolerant schemes for qudits of dimension other than 2, have not been studied as extensively as error correcting codes for qubits, though some interesting recent

work exists. We will focus on qudits of odd prime dimension, which are easy to study due to their mathematical properties. (See e.g., Appleby [37].)

Diagrammatic Approaches

Mathematicians, physicists and computer scientists have been representing mathematical structures graphically using nodes and wires for many years. Famously, Gilbreth and Gilbreth, in 1922 [26], introduced the idea of representing processes with flow chart. In physics, Feynman diagrams are one commonly-used diagrammatic technique. Penrose, in [27], released a particular class of diagrams that can be used to represent tensor calculus.

Paul Dirac gave a new notation for matrices and tensors in 1930 [28], called Dirac notation, and in 2005, Coecke [29] generalized Dirac notation and Penrose's graphical tensor calculus with the more abstract notation of states and effects in string diagrams. This framework can also be understood in the language of traced symmetric monoidal categories and evidence of correctness of graphical language for traced symmetric monoidal categories given by, e.g., Kissinger in 2014 [30]. Monoidal categories were first introduced in 1963 by Benabou [31]. Crucially related to monoidal categories to diagram is coherence proved by Mac Lane in 1963 [32]. Multilinear maps without fixing basis was described in 2004 by Penrose [33] which are used often in theoretical physics.

The approaches described here appear well suited to fault-tolerant quantum computing. We may also refer to [38] and [39].

The completeness and minimality of the ZX-calculus was addressed by Backens in [41],[42],[43] and [44].

The traditional language of Hilbert space is not very good at expressing many features of quantum theory, e.g. teleportation, entanglement. So, researchers and mathematicians such as Bob Coecke, have developed another appropriate language called processing theory. Purely diagrammatic approaches are unique methology that treats quantum processes and compositions of processes as basic building blocks [45].

In 2010, Bob Coecke defined Quantum picturalism [45]: “Quantum picturalism refers to the use of diagrams to represent, reason about, and capture essential features as well as the logic of interacting quantum processes, in a manner that these diagrammatic equations become the very foundation of quantum theory”.

OBJECTIVES

(1.) Approximate general unitary gates, for qudits, using Clifford and T gates for qudits instead of qubits.

(2.) Evaluate possible advantages of error-correcting codes and fault tolerant schemes based on qudits instead of qubits.

(3.) Develop new techniques using diagrammatic approaches

METHODOLOGY

Let us briefly illustrate the methodology we will use through some simple examples of error-correcting codes and diagrammatic calculus. A complete description will appear in the thesis.

Often, we use classical or quantum channels to transmit bits or qubits respectively. Due to noise in the channel or faulty gates, the transmitted data may have some error, so to correct the errors we use quantum or classical error-correcting codes. We can proceed from classical error correction codes to quantum error correction, which is useful because we are more familiar with classical error correction.

The Hamming code is one of the most important error correcting codes, and is widely used in classical error correction. So, let us briefly review it [34]:

Hamming codes:

Block codes [35]:-

Let us define a linear block code, which detects errors with rate $R=k/n$, through the parity check matrix $H = [h_1, h_2, h_3 \dots \dots \dots \dots h_n]$, which is a $(n-k) \times n$ matrix. The j^{th} column of H is h_j and has entries $h_{ij} \in GF(p)$, where $GF(p)$ is the finite field of integers with modulo p (where p is prime).

Definition:- The linear code $\mathcal{C}$ corresponding to the parity check matrix H is the set of codewords x such that

$$Hx = 0$$

In other words, the codewords $\mathcal{C}$ lie in the right null space of H.

A single error correcting code using parity matrix H, consisting of $2^m - 1$ columns of nonzero binary vectors of length $m=n-k$, corrects errors with rate $R = \frac{k}{n} = \frac{2^m - m - 1}{2^m - 1}$ and minimum distance $d_{min} = 3$.

$$H_{[7,4]} = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Each row of H is equivalent to a parity-check equation.

Illustration:

Hamming code using block code [7,4,3]:-

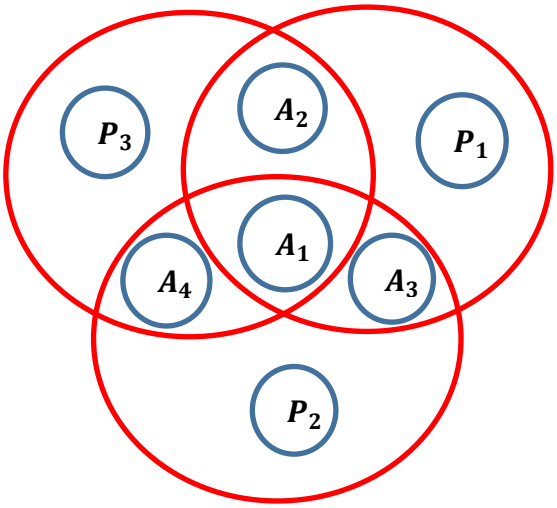
There code word consists of 7 bits, which are 4 bits of data $A_1A_2A_3A_4$ and 3 parity bits $P_1P_2P_3$. Using the below equation we can detect any single-bit error. Here $\oplus$ represents addition of modulo 2.

$$A_1 \oplus A_2 \oplus A_3 \oplus P_1 = 0$$

$$A_1 \oplus A_3 \oplus A_4 \oplus P_3 = 0$$

$$A_1 \oplus A_2 \oplus A_4 \oplus P_3 = 0$$

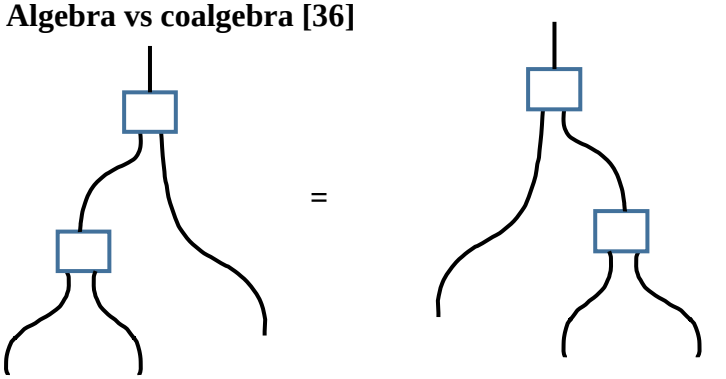
So if we represent each equation of parity-check using a circle then there should even numbers of 1's, as shown below:



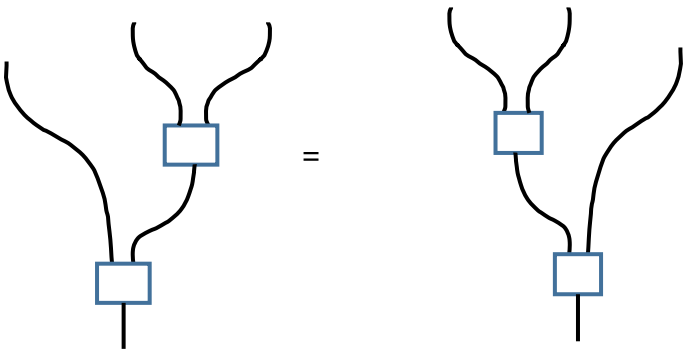
DIAGRAMMATIC APPROACHES ILLUSTRATION:

Here, we illustrate the diagrammatic approach of Bob Coecke, e.g., [36], briefly:

Algebra vs coalgebra [36]



associativity



coassociativity

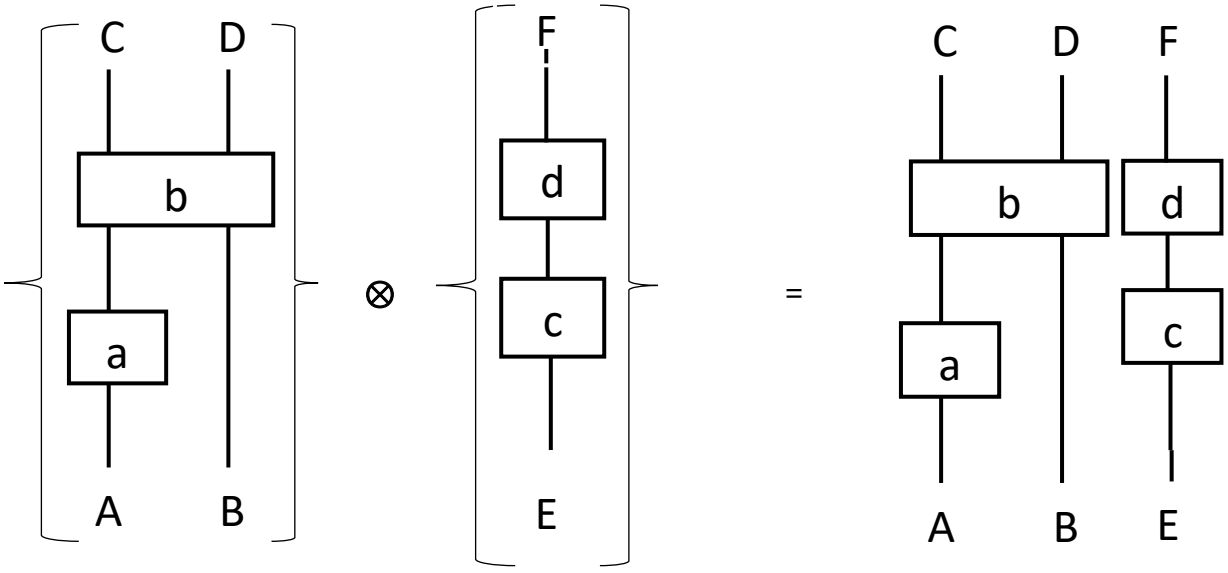
Circuit diagrams [36]:

Some basic structures of operation on process

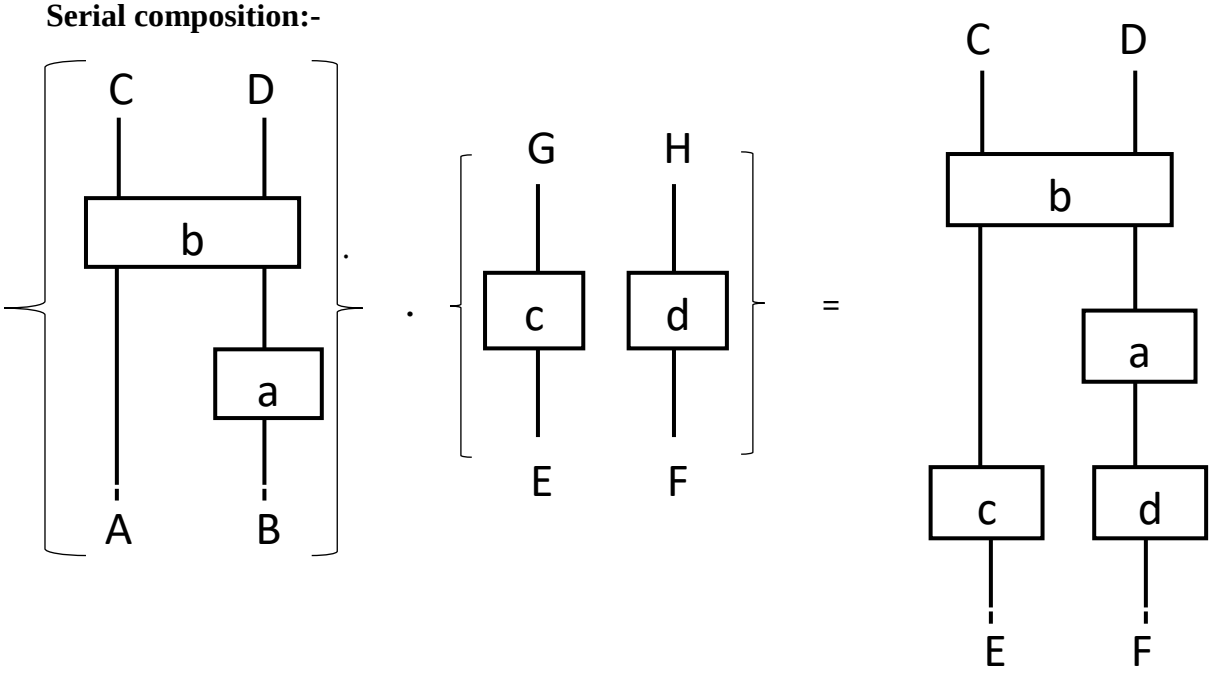
$$f \otimes g = Event\ f\ occur\ while\ g\ occur.$$

$$f \circ g = Event\ f\ occur\ after\ g.$$

Parallel composition:-

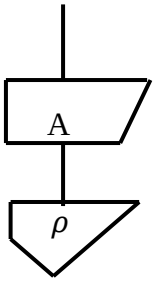


Serial composition:-



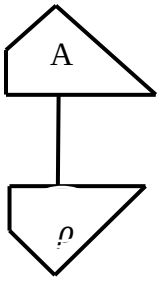
States correspond to density matrices:-

$$\varepsilon :: \rho \to \sum A_i^{\dagger} \rho A_i \;\; Depicted\ as:$$



Effect of positive linear functional:-

$\rho \to tr(A\rho)$ $Depicted\ as$:



REFERENCES

[1] R.P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6/7):467-488, 1982.

[2] P. Benio. Quantum mechanical models of Turing machines that dissipate no energy. *Physical Review Letters*, 48(23):1581-1585, 1982.

[3] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London, Series A*, 400(1818):97-117, 1985.

[4] D. Deutsch. Quantum computational networks. *Proceedings of the Royal Society of London, Series A,* 425(1868):73-90, 1989.

[5] A.C-C. Yao. Quantum circuit complexity. *In Proceedings of 34th Annual IEEE Symposium on Foundations of Computer Science,* pages 352-361, 1993.

[6] E. Bernstein and U. Vazirani. Quantum complexity theory. In STOC '93: *Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing,* pages 11-20,1993.

[7] A. Barenco, C.H. Bennett, R. Cleve, D.P. Di Vincenzo, N. Margolus, P.W. Shor,

T. Sleator, J.A. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Physical Review A,* 52(5):3457-3467, 1995.

[8] D.P. DiVincenzo. Two-bit gates are universal for quantum computation. *Physical Review A,* 51(2):1015-1022, 1995.

[9] A. Barenco, D. Deutsch, A. Ekert, and R. Jozsa. Conditional quantum dynamics and logic gates. *Physical Review Letters,* 74(20):4083-4086, 1995.

[10] S. Lloyd. Almost any quantum logic gate is universal. *Physical Review Letters,*

75(2):346-349, 1995.

[11] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London, Series A,* 439(1907):553-558, 1992.

[12] E. Bernstein and U. Vazirani. Quantum complexity theory. In STOC '93: *Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing,* pages 11-20,1993.

[13] P.W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring in *Foundations of Computer Science*, 1994, pp. 124–134.

[14] P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM Journal on Computing* 26 (1997), pp. 1484–1509.

[15] R.L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM* 21 (1978), pp. 120–126.

[16] L.K. Grover, A fast quantum mechanical algorithm for database search, in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 1996, pp. 212–219.

[17] M. Schuld, I. Sinayskiy, and F. Petruccione, An introduction to quantum machine learning, *Contemporary Physics* 56 (2015), pp. 172–185.

[18] K.L. Brown, W.J. Munro, and V.M. Kendon, Using quantum computers for quantum simulation, *Entropy* 12 (2010), pp. 2268–2307.

[19] P.W. Shor. Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, 52(4):R2493-R2496, 1995.

[20] A.M. Steane. Error correcting codes in quantum theory. *Physical Review Letters*, 77(5):793{797, 1996.

[21] A.R. Calderbank and P.W. Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098-1105, 1996.

[22] A.R. Calderbank and P.W. Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098-1105, 1996.

[23] B. Schumacher. Quantum coding. *Physical Review A*, 51(4):2738-2747, 1995.

[24] A. Barenco, D. Deutsch, A. Ekert, and R. Jozsa. Conditional quantum dynamics andlogic gates. *Physical Review Letters*, 74(20):4083{4086, 1995.

[25] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W.K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895-1899, March 1993.

[26] Gilbreth, F. B., and Gilbreth, L. M. 1922. Process charts and their place in management.Mechanical engineering, 70, 38{41.

[27] Penrose, R. 1971. Applications of negative dimensional tensors. Pages 221-244 of *Combinatorial Mathematics and its Applications*. Academic Press.

[28] Dirac, P. A. M. 1939. A new notation for quantum mechanics. Pages 416-418 of *Proceedings of the Cambridge Philosophical Society*, vol. 35. Cambridge Univ Press.

[29] Coecke, B. 2005. Kindergarten quantum mechanics. Pages 81{98 of: Khrennikov,A. (ed), Quantum Theory: Reconsiderations of the Foundations III. AIP Press.arXiv:quant-ph/0510032.

[30] Kissinger, A. 2014a. Abstract tensor systems as monoidal categories. In: Casadio,C, Coecke, B, Moortgat, M, and Scott, P (eds), Categories and Types in *Logic, Language, and Physics: Festschrift on the occasion of Jim Lambek's 90th birthday. Lecture Notes in Computer Science*, vol. 8222. Springer. arXiv:1308.3586.

[31] Benabou, J. 1963. Categories avec multiplication. Comptes Rendus des Seances del'Academie des Sciences. Paris, 256, 1887{1890.

[32] Mac Lane, S. 1963. Natural associativity and commutativity. The Rice University Studies, 49(4), 28{46.

[33] Penrose, R. 2004. The Road to Reality: A Complete Guide to the Physical Universe.Jonathan Cape.

[34] H. Nickl, J. Hagenauer, and F. Burkert, “Approaching Shannon’s capacity limit by 0.27 dB using simple Hamming codes,” *IEEE Commun. Lett.*, vol. 1, no. 5, Sept. 1997.

[35] T. Taneko, T. Nishijima, H. Inazumi, and S. Hirasawa, “Efficient maximum likelihood decoding of linear block codes with algebraic decoder,” *IEEE Trans. Inform. Theory*, vol. IT-40, pp. 320–327, March 1994.

[36] Joyal, A., and Street, R. 1991. “The geometry of tensor calculus I,” Advances in Mathematics, 88, 55(112).

[37] Appleby, D. M. "Properties of the extended Clifford group with applications to SIC-POVMs and MUBs." arXiv preprint arXiv:0909.5233 (2009).

[38] Srivastava, Dayal Pyari, Vishal Sahni, and Prem Saran Satsangi. "Graph-theoretic quantum system modelling for information/computation processing circuits." *International Journal of General Systems* 40.8 (2011): 777-804.

[39] Srivastava, Dayal Pyari, Vishal Sahni, and Prem Saran Satsangi. "Graph-theoretic quantum system modelling for information/computation processing circuits." *International Journal of General Systems* 40.8 (2011): 777-804.

[40] Srivastava, Dayal Pyari, Vishal Sahni, and Prem Saran Satsangi. "Modelling microtubules in the brain as n-qudit quantum Hopfield network and beyond." *International Journal of General Systems* 45.1 (2016): 41-54.

[41] Backens, M. 2014a The ZX-calculus is complete for stabilizer quantum mechanics. *New journal of physics*, 16, 093021. arXiv:1307.7025.

[42] Backens, M. 2014b. *The ZX-calculus is complete for the single -qubit Clifford+T group*. arXiv:1412.8553.

[43] Backens, M., prefix, S., and Wang, Q. 2016. *Soundness, completeness, and minimality of the stabiliser ZX-calculus*. Forthcoming.

[44] Backens, M., Perdrix, S. and Wang, Q., 2017. Towards a Minimal Stabilizer ZX-calculus. *arXiv preprint arXiv:1709.08903*.

[45] Coecke, B., 2010. Quantum picturalism. *Contemporary physics*, *51*(1), pp.59-83.